THAT WHICH IS CLAIMED:

1. A system for controlling access to digital data of a file, the system comprising:

a file server configured to store an encrypted file and a file header corresponding to the digital data of the file and containing an encryption key encrypted with both a personal key of an owner of the file and a control key;

a personal key server configured to receive a header associated with a file, the file header containing an encryption key encrypted with a personal key and encrypt encrypted encryption key with a control key to provide the file header containing an encryption key encrypted with both a personal key and a control key; and

a personal key client configured to generate the encryption key, encrypt the digital data of the file with the encryption key, generate the personal key from a password associated with the file, encrypt the encryption key with the personal key, incorporate the encrypted encryption key in a file header associated with the file and provide the file header with the encryption key encrypted with the personal key to the personal key server, receive the file header from the personal key server and provide the file header received from the personal key server to the file server.

2. A system according to Claim 1, further comprising:

an authentication server configured to receive access requests from the personal key client, determine if the access request is authorized and provide a ticket to the personal key client if the access request is authorized;

wherein the personal key client is further configured to request access from the authentication server, receive the ticket from the authentication server and provide the ticket along with the file header to the personal key server and along with the encrypted file and the file header to the file server;

wherein the personal key server is further configured to receive the ticket from the personal key client, determine the validity of the ticket and reject requests from the personal key client if the ticket is invalid; and

wherein the file server is further configured to receive the ticket from the personal key client, determine the validity of the ticket and reject requests from the personal key client if the ticket is invalid.

3. A system according to Claim 1, wherein the personal key client is further configured to receive a request to access the file by the file owner, request the file and the associated file header from the file server, extract the encryption key encrypted with the personal key and the control key from the file header, request that the personal key server recover the encrypted encryption key from the file header, receive the recovered encrypted encryption key from the personal key server, generate the personal key from the password, decrypt the recovered encrypted encryption key with the personal key to recover the encryption key and decrypt the encrypted digital data with the recovered encryption key;

wherein the file server is configured to provide the file and the associated file header in to the personal key client in response to the request for the file and the associated file header; and

wherein the personal key server is configured to receive a request from the personal key client to recover the encrypted encryption key containing the encryption key encrypted with the personal key and the control key, decrypt the encryption key encrypted with the personal key and the control key with the control key and return the encryption key encrypted with the personal key to the personal key client.

4. A system according to 1, wherein the personal key client is further configured to request the file header associated with the file from the file server, receive the file header from the file server, extract the encryption key encrypted with the personal key and the control key, request that the personal key server recover the encrypted encryption key, receive the recovered encrypted encryption key from the personal key server, generate the personal key, decrypt the recovered encrypted encryption key with the personal key to provide a recovered encryption key, obtain a new password associated with the file, generate a new personal key based on the new password, encrypt the recovered encryption key to provide a new personal key encrypted encryption key, request an update of the file header by the personal key server to incorporate the new personal key encrypted encryption key, receive an updated file header from the personal key server and provide the updated file header to the file server;

wherein the file server is configured to receive the request for the file header from the personal key client, provide the file header to the personal key client, receive the updated file header from the personal key client and store the received file header; and

wherein the personal key server is configured to receive the request to recover the encrypted file encryption key, decrypt the file encryption key encrypted with the personal key and the control key to provide the recovered encrypted encryption key, provide the recovered encrypted encryption key to the personal key client, receive the request to update the file header to incorporate the new personal key encrypted encryption key, encrypt the new personal key encrypted encryption key with the control key, incorporate the encryption key encrypted with the new personal key and the control key in the file header to provide an updated file header and return the updated file header to the personal key client.

5. A system according to Claim 4 wherein the personal key client is further configured to include in the request to update of the file header by the personal key server an identification of a user requesting to update the file header; and

wherein the personal key server if further configured to compare the identification of the user requesting to update the file header with a list of users authorized to access the file and reject the request if the user requesting to update the file header is not identified in the list of users authorized to access the file as the owner of the file.

6. A system according to Claim 1, wherein the personal key client is further configured to encrypt the encryption key with a public key of a trusted third party and incorporate the encryption key encrypted with the public key of a trusted third party into the file header.

7. A system according to Claim 6, wherein the personal key client is further configured to receive a request by the trusted third party to access the file, request access to the file by the trusted third party from the file server, receive the encrypted file and the file header from the file server, extract the encryption key encrypted with the public key of the trusted third party from the received file header, obtain the private key of the trusted third party, decrypt the extracted encryption key encrypted with the public key of the trusted third party to recover the encryption key and decrypt the encrypted file with the recovered encryption key; and

wherein the file server is further configured to receive the request for access to the file by the trusted third party and provide the encrypted file and the associated file header to the personal key client in response to receiving the request for access to the file by the trusted third party.

8. A system according to Claim 6, wherein the personal key client is further configured to request the file header associated with the file from the file server, receive the file header from the file server, extract the encryption key encrypted with the personal key and the control key, request that the personal key server recover the encrypted encryption key, receive the recovered encrypted encryption key from the personal key server, generate the personal key, decrypt the recovered encrypted encryption key with the personal key, obtain a new public key associated with the trusted third party to provide a new public key encrypted encryption key, incorporate the new public key encryption key in the file header and provide the file header to the file server;

wherein the file server is configured to receive the request for the file header from the personal key client, provide the file header to the personal key client, receive the file header from the personal key client and store the received file header; and

wherein the personal key server is configured to receive the request to recover the encrypted file encryption key, decrypt the file encryption key encrypted with the personal key and the control key to provide the recovered encrypted encryption key and provide the recovered encrypted encryption key to the personal key client.

9. A system according to Claim 1, wherein the personal key client is further configured to incorporate the encryption key unencrypted in the file header and to provide the personal key server with a list of users authorized to have access to the file; and

wherein the personal key server is further configured to encrypt the unencrypted encryption key with the control key, and incorporate the unencrypted encryption key encrypted with the control key in the file header and return the file header incorporating the encryption key encrypted with the control key to the personal key client.

10. A system according to Claim 9, wherein the personal key client is further configured to receive a request to access the file by a user other than the file owner, request the file and the associated file header from the file server, extract the encryption key encrypted with only the control key from the file header, request that the personal key server recover the encryption key from the file header, receive the

recovered encryption key from the personal key server and decrypt the encrypted digital data with the recovered encryption key;

wherein the file server is configured to provide the file and the associated file header in to the personal key client in response to the request for the file and the associated file header; and

wherein the personal key server is configured to receive a request from the personal key client to recover the encryption key in response to a request by a user other than the owner, the request from the personal key client containing the encryption key encrypted with the control key, decrypt the encryption key encrypted with the control key with the control key and return the encryption key to the personal key client.

11. A system according to Claim 10 wherein the personal key client is further configured to include in the request to recover the encryption key an identification of the user requesting to access the file; and

wherein the personal key server if further configured to compare the identification of the user requesting to access the file with the list of users authorized to access the file and reject the request if the user requesting to access the file is not identified in the list of users authorized to access the file.

12. A system according to Claim 1, wherein the personal key client is further configured to encrypt the encryption key with a public key of each user other than the owner which are authorized to access the file to provide a public key encrypted encryption key

corresponding to each user other than the owner, incorporate the public key encrypted encryption key corresponding to each user other than the owner of the file in the file header and to provide the personal key server with a list containing each user authorized to have access to the file; and

wherein the personal key server is further configured to encrypt each public key encrypted encryption key with the control key, and incorporate each public key encrypted encryption key encrypted with the control key in the file header and return the file header incorporating each public key encrypted encryption key encrypted with the control key to the personal key client.

13. A system according to 12, wherein the personal key client is further configured to request the file header associated with the file from the file server, receive the file header from the file server, extract the encryption key encrypted with the personal key and the control key, request that the personal key server recover the encrypted encryption key, receive the recovered encrypted encryption key from the personal key server, generate the personal key, decrypt the recovered encrypted encryption key with the personal key to provide a recovered encryption key, obtain a new public key associated with a user other than the owner of the file, encrypt the recovered encryption key with the new public key to provide a new public key encrypted encryption key, request an update of the file header by the personal key server to incorporate the new public key encrypted encryption key, receive an updated file header from the personal key server and provide the updated file header to the file server;

wherein the file server is configured to receive the request for the file header from the personal key client, provide the file header to the personal key client, receive the updated file header from the personal key client and store the received file header; and

wherein the personal key server is configured to receive the request to recover the encrypted file encryption key, decrypt the file encryption key encrypted with the personal key and the control key to provide the recovered encrypted encryption key, provide the recovered encrypted encryption key to the personal key client, receive the request to update the file header to incorporate the new public key encrypted encryption key, encrypt the new public key encrypted encryption key with the control key, incorporate the encryption key encrypted with the new public key and the control key in the file header to provide an updated file header and return the updated file header to the personal key client.

14. A system according to Claim 12 wherein the personal key client is further configured to include in the request to update of the file header by the personal key server to incorporate the new public key encrypted encryption key an identification of a user requesting to update the file header; and

wherein the personal key server is further configured to compare the identification of the user requesting to update the file header with the list of users authorized to access the file and reject the request if the user requesting to update the file header is not identified in the list of users authorized to access the file as the owner of the file.

15. A system according to Claim 12 wherein the personal key client is further configured to receive a request from a user other than the owner to access the file, request the file and the associated file header from the file server, extract the public key encrypted encryption key encrypted with the control key corresponding to the user requesting access to the file from the file header, request that the personal key server recover the public key encrypted encryption key corresponding to the user requesting access to the file from the file header, receive the recovered public key encrypted encryption key from the personal key server, obtain a private key associated with the user requesting access to the file, decrypt the recovered encrypted encryption key with the private key to recover the encryption key and decrypt the encrypted digital data with the recovered encryption key;

wherein the file server is configured to provide the file and the associated file header in to the personal key client in response to the request for the file and the associated file header; and

wherein the personal key server is configured to receive a request from the personal key client to recover the public key encrypted encryption key containing the public key encrypted encryption key encrypted with the control key corresponding to the user requesting access to the file, decrypt the public key encrypted encryption key encrypted the control key with the control key and return the public key encrypted encryption key corresponding to the user requesting the file to the personal key client.

16. A system according to Claim 15 wherein the personal key client is further configured to include in the request to recover the public key encrypted

encryption key corresponding to the user requesting to access the file an identification of the user requesting to access the file; and

wherein the personal key server is further configured to compare the identification of the user requesting to access the file with the list of users authorized to access the file and reject the request if the user requesting to access the file is not identified in the list of users authorized to access the file.

17. A method for controlling access to digital data of a file utilizing a file system including a personal key client, wherein the personal key client carries out the steps of:

generating an encryption key;

encrypting the digital data of the file with the encryption key;

obtaining a password associated with the file;

generating a personal key from the password associated with the file;

encrypting the encryption key with the personal key;

incorporating in a file header the encryption key encrypted with the personal key;

requesting encryption of the file header with a control key;

receiving the file header encrypted with the control key;

associating the file header with the file; and

storing the file header and the encrypted digital data of the file at a file server.

18. A method according to Claim 17, further comprising:

receiving access requests from a user to access the file system;

determining if the access request is authorized;

providing a ticket utilized to access the file system if the access request is authorized; and

utilizing the ticket to perform file storage, access and administrative operations.

19. A method according to Claim 17, further comprising the steps of:

receiving a request to access the file by the file owner;

requesting the file and the associated file header from the file server;

extracting the encryption key encrypted with the personal key and the control key from the file header;

requesting recovery of the encrypted encryption key from the file header;

receiving the recovered encrypted encryption key;

obtaining a password to decrypt the file;

generating the personal key from the obtained password;

decrypting the recovered encrypted encryption key with the personal key to recover the encryption key; and

decrypting the encrypted digital data with the recovered encryption key.

20. A method according to 17, further comprising the steps of:

requesting the file header associated with the file from the file server;

receiving the file header from the file server;

extracting the encryption key encrypted with the personal key and the control key;

requesting recovery of the encrypted encryption key;

receiving the recovered encrypted encryption key;

generating the personal key;

decrypting the recovered encrypted encryption key with the personal key to provide a recovered encryption key;

obtaining a new password associated with the file;

generating a new personal key based on the new password;

encrypting the recovered encryption key to provide a new personal key encrypted encryption key;

requesting an update of the file header to incorporate the new personal key encrypted encryption key;

receiving an updated file header from the personal key server; and

providing the updated file header to the file server.

21. A method according to Claim 17, further comprising:

encrypting the encryption key with a public key of a trusted third party;

incorporating the encryption key encrypted with the public key of a trusted third party into the received file header to provide a new file header; and

storing the new file header at the file server.

22. A method according to Claim 21, further comprising:

receiving a request by the trusted third party to access the file;

requesting access to the file by the trusted third party from the file server;

receiving the encrypted file and the file header from the file server;

extracting the encryption key encrypted with the public key of the trusted third party from the received file header;

obtaining the private key of the trusted third party;

decrypting the extracted encryption key encrypted with the public key of the trusted third party to recover the encryption key; and

decrypting the encrypted file with the recovered encryption key.

23. A method according to Claim 21, further comprising:

requesting the file header associated with the file from the file server;

receiving the file header from the file server;

extracting the encryption key encrypted with the personal key and the control key;

requesting recovery of the encrypted encryption key;

receiving the recovered encrypted encryption key;

generating the personal key;

decrypting the recovered encrypted encryption key with the personal key to provide a recovered encryption key;

obtaining a new public key associated with the trusted third party;

encrypting the recovered encryption key with the new public key to provide a new public key encrypted encryption key;

incorporating the new public key encryption key in the file header to provide an updated file header; and

providing the updated file header to the file server.

24. A method according to Claim 17, wherein the step of requesting encryption of the file header with a control key is preceded by the step of incorporating the encryption key unencrypted in the file header; and the method further comprising:

providing a list of users authorized to have access to the file.

25. A method according to Claim 24, further comprising:

receiving a request to access the file by a user other than the file owner;

requesting the file and the associated file header from the file server;

extracting the encryption key encrypted with only a control key from the file header;

requesting recovery of the encryption key from the file header;

receiving the recovered encryption key; and

decrypting the encrypted digital data with the recovered encryption key.

26. A method according to Claim 17, wherein the step of requesting encryption of the file header with a control key is preceded by the steps of:

encrypting the encryption key with a public key of each user other than the owner which is authorized to access the file to provide a public key encrypted encryption key corresponding to each user other than the owner;

incorporating the public key encrypted encryption key corresponding to each user other than the owner of

the file in the file header; and the method further comprising:

providing a list containing each user authorized to have access to the file.

27. A method according to 26, further comprising:

requesting the file header associated with the file from the file server;

receiving the file header from the file server;

extracting the encryption key encrypted with the personal key and the control key from the received file header;

requesting recovery of the encrypted encryption key;

receiving the recovered encrypted encryption key;

generating the personal key;

decrypting the recovered encrypted encryption key with the personal key to provide a recovered encryption key;

obtaining a new public key associated with a user other than the owner of the file;

encrypting the recovered encryption key with the new public key to provide a new public key encrypted encryption key;

requesting an update of the file header to incorporate the new public key encrypted encryption key;

receiving an updated file header; and

providing the updated file header to the file server.

28. A method according to Claim 26 further comprising:

receiving a request from a user other than the owner to access the file;

requesting the file and the associated file header from the file server;

receiving the encrypted file and the file header form the file server;

extracting the public key encrypted encryption key encrypted with the control key corresponding to the user requesting access to the file from the file header;

requesting recovery of the public key encrypted encryption key corresponding to the user requesting access to the file from the file header;

receiving the recovered public key encrypted encryption key;

obtaining a private key associated with the user requesting access to the file;

decrypting the recovered encrypted encryption key with the private key to recover the encryption key; and

decrypting the encrypted digital data with the recovered encryption key.

29. A method for controlling access to digital data of a file in a file system having a personal key server, the personal key server carrying out the steps of:

receiving a request from a requestor to create a file header associated with the file, the request containing an encryption key encrypted with a personal key;

encrypting the encrypted encryption key with a control key to provide the file header containing an encryption key encrypted with both a personal key and a control key; and

returning the file header to the requestor.

30. A method according to Claim 29, wherein the request further includes an authentication ticket, the method further comprising the steps of:

determining the validity of the authentication ticket; and

rejecting the request if the authentication ticket is invalid.

31. A method according to Claim 29, further comprising:

receiving a request from the personal key client to recover the encrypted encryption key containing the encryption key encrypted with the personal key and the control key;

decrypting the encryption key encrypted with the personal key and the control key with the control key;

returning the encryption key encrypted with the personal key.

32. A method according to 29, further comprising:

receiving a request to update the file header to incorporate an encryption key encrypted with a new encryption key;

encrypting the encryption key encrypted with the new encryption key with the control key to provide a control key encrypted new encryption key encrypted encryption key;

incorporating the control key encrypted new encryption key encrypted encryption key in the file header to provide an updated file header; and

returning the updated file header.

33. A method according to Claim 32, wherein the request to update of the file header to incorporate the encryption key encrypted with a new encryption key

includes an identification of a user requesting to update the file header, the method further comprising:

comparing the identification of the user requesting to update the file header with a list of users authorized to access the file; and

rejecting the request if the user requesting to update the file header is not identified in the list of users authorized to access the file as the owner of the file.

34. A method according to Claim 29, wherein the request from a requestor to create a file header associated with the file, further contains an unencrypted encryption key associated with users authorized to access the file, the method further comprising:

encrypting the unencrypted encryption key with the control key;

incorporating the unencrypted encryption key encrypted with the control key in the file header; and

returning the file header incorporating the encryption key encrypted with the control key.

35. A method according to Claim 34, further comprising:

receiving a request to recover the encryption key in response to a request by a user other than an owner of the file containing the encryption key encrypted with the control key;

decrypting the encryption key encrypted with the control key with the control key; and

returning the encryption key.

36. A method according to Claim 35 wherein the request to recover the encryption key includes an

identification of the user requesting to access the file, the method further comprising:

comparing the identification of the user requesting to access the file with a list of users authorized to access the file; and

rejecting the request if the user requesting to access the file is not identified in the list of users authorized to access the file.

37. A system according to Claim 29, wherein the request to create a file header associated with the file includes a public key encrypted encryption key corresponding to each user authorized to access the file other than an owner of the file and a list containing each user authorized to have access to the file, the method further comprising:

encrypting each public key encrypted encryption key with the control key;

incorporating each public key encrypted encryption key encrypted with the control key in the file header;

returning the file header incorporating each public key encrypted encryption key encrypted with the control key.

38. A method according to Claim 37, further comprising the step of creating an access control list from the list provided with the request.

39. A method according to Claim 37, further comprising:

receiving a request to recover the public key encrypted encryption key containing the public key encrypted encryption key encrypted with the control key corresponding to a user requesting access to the file;

decrypting the public key encrypted encryption key encrypted the control key with the control key; and

returning the public key encrypted encryption key corresponding to the user requesting the file.

40. A method according to Claim 39, further comprising:

comparing the identification of the user requesting to access the file with the list of users authorized to access the file; and

rejecting the request if the user requesting to access the file is not identified in the list of users authorized to access the file.

41. A personal key client for controlling access to digital data of a file utilizing a file system, comprising:

means for generating an encryption key;

means for encrypting the digital data of the file with the encryption key;

means for obtaining a password associated with the file;

means for generating a personal key from the password associated with the file;

means for encrypting the encryption key with the personal key;

means for incorporating in a file header the encryption key encrypted with the personal key;

means for requesting encryption of the file header with a control key;

means for receiving the file header encrypted with the control key;

means for associating the file header with the file; and

means for storing the file header and the encrypted digital data of the file at a file server.

42. A personal key client according to Claim 41, further comprising:

means for receiving access requests from a user to access the file system;

means for determining if the access request is authorized;

means for providing a ticket utilized to access the file system if the access request is authorized; and

means for utilizing the ticket to perform file storage, access and administrative operations.

43. A personal key client according to Claim 41, further comprising:

means for receiving a request to access the file by the file owner;

means for requesting the file and the associated file header from the file server;

means for extracting the encryption key encrypted with the personal key and the control key from the file header;

means for requesting recovery of the encrypted encryption key from the file header;

means for receiving the recovered encrypted encryption key;

means for obtaining a password to decrypt the file;

means for generating the personal key from the obtained password;

means for decrypting the recovered encrypted encryption key with the personal key to recover the encryption key; and

means for decrypting the encrypted digital data with the recovered encryption key.

44. A personal key client according to 41, further comprising:

means for requesting the file header associated with the file from the file server;

means for receiving the file header from the file server;

means for extracting the encryption key encrypted with the personal key and the control key;

means for requesting recovery of the encrypted encryption key;

means for receiving the recovered encrypted encryption key;

means for generating the personal key;

means for decrypting the recovered encrypted encryption key with the personal key to provide a recovered encryption key;

means for obtaining a new password associated with the file;

means for generating a new personal key based on the new password;

means for encrypting the recovered encryption key to provide a new personal key encrypted encryption key;

means for requesting an update of the file header to incorporate the new personal key encrypted encryption key;

means for receiving an updated file header from the personal key server; and

means for providing the updated file header to the file server.

45. A personal key client according to Claim 41, further comprising:

means for encrypting the encryption key with a public key of a trusted third party;

means for incorporating the encryption key encrypted with the public key of a trusted third party into the received file header to provide a new file header; and

means for storing the new file header at the file server.

46. A personal key client according to Claim 45, further comprising:

means for receiving a request by the trusted third party to access the file;

means for requesting access to the file by the trusted third party from the file server;

means for receiving the encrypted file and the file header from the file server;

means for extracting the encryption key encrypted with the public key of the trusted third party from the received file header;

means for obtaining the private key of the trusted third party;

means for decrypting the extracted encryption key encrypted with the public key of the trusted third party to recover the encryption key; and

means for decrypting the encrypted file with the recovered encryption key.

47. A personal key client according to Claim 45, further comprising:

means for requesting the file header associated with the file from the file server;

means for receiving the file header from the file server;

means for extracting the encryption key encrypted with the personal key and the control key;

means for requesting recovery of the encrypted encryption key;

means for receiving the recovered encrypted encryption key;

means for generating the personal key;

means for decrypting the recovered encrypted encryption key with the personal key to provide a recovered encryption key;

means for obtaining a new public key associated with the trusted third party;

means for encrypting the recovered encryption key with the new public key to provide a new public key encrypted encryption key;

means for incorporating the new public key encryption key in the file header to provide an updated file header; and

means for providing the updated file header to the file server.

48. A personal key client according to Claim 41, further comprising:

means for incorporating the encryption key unencrypted in the file header; and

means for providing a list of users authorized to have access to the file.

49. A personal key client according to Claim 48, further comprising:

means for receiving a request to access the file by a user other than the file owner;

means for requesting the file and the associated file header from the file server;

means for extracting the encryption key encrypted with only a control key from the file header;

means for requesting recovery of the encryption key from the file header;

means for receiving the recovered encryption key; and

means for decrypting the encrypted digital data with the recovered encryption key.

50. A personal key client according to Claim 41, further comprising:

means for encrypting the encryption key with a public key of each user other than the owner which is authorized to access the file to provide a public key encrypted encryption key corresponding to each user other than the owner;

means for incorporating the public key encrypted encryption key corresponding to each user other than the owner of the file in the file header; and

means for providing a list containing each user authorized to have access to the file.

51. A personal key client according to 50, further comprising:

means for requesting the file header associated with the file from the file server;

means for receiving the file header from the file server;

means for extracting the encryption key encrypted with the personal key and the control key from the received file header;

means for requesting recovery of the encrypted encryption key;

means for receiving the recovered encrypted encryption key;

means for generating the personal key;

means for decrypting the recovered encrypted encryption key with the personal key to provide a recovered encryption key;

means for obtaining a new public key associated with a user other than the owner of the file;

means for encrypting the recovered encryption key with the new public key to provide a new public key encrypted encryption key;

means for requesting an update of the file header to incorporate the new public key encrypted encryption key;

means for receiving an updated file header; and

means for providing the updated file header to the file server.

52. A personal key client according to Claim 50 further comprising:

means for receiving a request from a user other than the owner to access the file;

means for requesting the file and the associated file header from the file server;

means for receiving the encrypted file and the file header form the file server;

means for extracting the public key encrypted encryption key encrypted with the control key corresponding to the user requesting access to the file from the file header;

means for requesting recovery of the public key encrypted encryption key corresponding to the user requesting access to the file from the file header;

means for receiving the recovered public key encrypted encryption key;

means for obtaining a private key associated with the user requesting access to the file;

means for decrypting the recovered encrypted encryption key with the private key to recover the encryption key; and

means for decrypting the encrypted digital data with the recovered encryption key.

53. A personal key server for controlling access to digital data of a file in a file system having a personal key server, comprising:

means for receiving a request from a requestor to create a file header associated with the file, the request containing an encryption key encrypted with a personal key;

means for encrypting the encrypted encryption key with a control key to provide the file header containing an encryption key encrypted with both a personal key and a control key; and

means for returning the file header to the requestor.

54. A personal key server according to Claim 53, wherein the request further includes an authentication ticket, the personal key server further comprising:

means for determining the validity of the authentication ticket; and

means for rejecting the request if the authentication ticket is invalid.

55. A personal key server according to Claim 53, further comprising:

means for receiving a request from the personal key client to recover the encrypted encryption key containing the encryption key encrypted with the personal key and the control key;

means for decrypting the encryption key encrypted with the personal key and the control key with the control key;

means for returning the encryption key encrypted with the personal key.

56. A personal key server according to 53, further comprising:

means for receiving a request to update the file header to incorporate an encryption key encrypted with a new encryption key;

means for encrypting the encryption key encrypted with the new encryption key with the control key to provide a control key encrypted new encryption key encrypted encryption key;

means for incorporating the control key encrypted new encryption key encrypted encryption key in the file header to provide an updated file header; and

means for returning the updated file header.

57. A personal key server according to Claim 56, wherein the request to update of the file header to incorporate the encryption key encrypted with a new encryption key includes an identification of a user requesting to update the file header, the personal key server further comprising:

means for comparing the identification of the user requesting to update the file header with a list of users authorized to access the file; and

means for rejecting the request if the user requesting to update the file header is not identified in the list of users authorized to access the file as the owner of the file.

58. A personal key server according to Claim 53, wherein the request from a requestor to create a file header associated with the file further contains an unencrypted encryption key associated with users authorized to access the file, the personal key server further comprising:

means for encrypting the unencrypted encryption key with the control key;

means for incorporating the unencrypted encryption key encrypted with the control key in the file header; and

means for returning the file header incorporating the encryption key encrypted with the control key.

59. A personal key server according to Claim 58, further comprising:

means for receiving a request to recover the encryption key in response to a request by a user other than an owner of the file containing the encryption key encrypted with the control key;

means for decrypting the encryption key encrypted with the control key with the control key; and

means for returning the encryption key.

60. A personal key server according to Claim 59 wherein the request to recover the encryption key includes an identification of the user requesting to access the file, the personal key server further comprising:

means for comparing the identification of the user requesting to access the file with a list of users authorized to access the file; and

means for rejecting the request if the user requesting to access the file is not identified in the list of users authorized to access the file.

61. A personal key server according to Claim 53, wherein the request to create a file header associated with the file includes a public key encrypted encryption key corresponding to each user authorized to access the file other than an owner of the file and a list containing each user authorized to have access to the file, the personal key server further comprising:

means for encrypting each public key encrypted encryption key with the control key;

means for incorporating each public key encrypted encryption key encrypted with the control key in the file header; and

means for returning the file header incorporating each public key encrypted encryption key encrypted with the control key.

62. A personal key server according to Claim 61, further comprising means for creating an access control list from the list provided with the request.

63. A personal key server according to Claim 61, further comprising:

means for receiving a request to recover the public key encrypted encryption key containing the public key encrypted encryption key encrypted with the control key corresponding to a user requesting access to the file;

means for decrypting the public key encrypted encryption key encrypted the control key with the control key; and

means for returning the public key encrypted encryption key corresponding to the user requesting the file.

64. A personal key server according to Claim 63, further comprising:

means for comparing the identification of the user requesting to access the file with the list of users authorized to access the file; and

means for rejecting the request if the user requesting to access the file is not identified in the list of users authorized to access the file.

65. A computer program product for controlling access to digital data of a file utilizing a file system including a personal key client, comprising:

a computer readable storage media having computer readable program code embodied therein, the computer readable program code comprising:

computer readable program code that generates an encryption key;

computer readable program code that encrypts the digital data of the file with the encryption key;

computer readable program code that obtains a password associated with the file;

computer readable program code that generates a personal key from the password associated with the file;

computer readable program code that encrypts the encryption key with the personal key;

computer readable program code that incorporates in a file header the encryption key encrypted with the personal key;

computer readable program code that requests encryption of the file header with a control key;

computer readable program code that receives the file header encrypted with the control key;

computer readable program code that associates the file header with the file; and

computer readable program code that stores the file header and the encrypted digital data of the file at a file server.

66. A computer program product for controlling access to digital data of a file in a file system having a personal key server, comprising:

computer readable program code that receives a request from a requestor to create a file header associated with the file, the request containing an encryption key encrypted with a personal key;

computer readable program code that encrypts the encrypted encryption key with a control key to provide the file header containing an encryption key encrypted with both a personal key and a control key; and

computer readable program code that returns the file header to the requestor.